

Seminar
Klassische Gruppen

**Räume über
endliche Körper**

Torsten Sprenger
sprenger@mathematik.uni-kassel.de
www.mathematik.uni-kassel.de/~sprenger

9. Juli 2003

21 Räume über endliche Körper

In diesem Abschnitt gelten folgende Voraussetzungen:

F sei ein endlicher Körper der Charakteristik p und V sei ein orthogonaler, symplektischer oder unitärer Vektorraum über F . Die Dimension von V sei n . Zunächst gilt folgender Hilfssatz, den man für **Beweis 21.1** und **21.3** benötigt:

Hilfssatz 1 *Jedes Element $a \in F$ lässt sich schreiben als $a = x^2 + y^2$ mit geeigneten $x, y \in F$.*

Beweis

1. Sei $\text{char}(F) = 2$. Beh.: Jedes Element ist Quadrat.
Ann.: Es existiert ein Element, das kein Quadrat ist.
 $\Rightarrow \exists a, b \in F$ mit $a \neq b$ und $a^2 = b^2$. $\Rightarrow b^2 - a^2 = (b+a)(b-a) = 0$.
 Es folgt somit $b = a$ oder $b = -a$. Da aber $\text{char}(F) = 2$, ist $a = -a$ und der zweite Fall mit dem ersten Fall identisch. Widerspruch zu $a \neq b$.
2. Sei $\text{char}(F) \neq 2$. Ferner sei A die Menge aller Quadrate von $F^\#$, also $A := \{a^2 \mid a \in F^\#\}$ und k ein Nichtquadrat. Es gilt $F^\# = A \cup Ak$.
 - $b = 0 : 0 = 0^2 + 0^2$
 - $b \in A : \exists c \in F^\#$ mit $b = c^2 = c^2 + 0^2$
 - $b \in Ak :$
Bem.: Ist $ck = x^2 + y^2$ für ein $c \in A$ und sei $c' \in A$ bel.
 $\Rightarrow \exists a \in F^\#$ mit $c' = a^2c$ und $c'k = a^2ck = a^2(x^2 + y^2) = (ax)^2 + (ay)^2$
 Es genügt also zu zeigen, daß unter den Elementen der Gestalt $x^2 + y^2$ ein Nichtquadrat ist.
Ann.: $\forall x, y \in F$ ist $x^2 + y^2$ Quadrat
 $\Rightarrow G := \{0\} \cup A$ ist Teilkörper von F .
 Sei $|F| = q \Rightarrow |G| = 1 + \frac{q-1}{2} = \frac{q+1}{2}$
 $\Rightarrow \frac{q+1}{2}$ ist kein Teiler von q , was aber dem Satz von Lagrange widerspricht.

□

Satz 21.1 *Sei $n = 2$. Dann existiert eine (bis auf Äquivalenz) eindeutige, nicht ausgeartete quadratische Form Q auf V . Ferner gibt es eine Basis $X = \{x, y\}$ von V , so daß folgendes gilt:*

1. Wenn p ungerade ist, dann ist
 $(x, y) = 0, Q(x) = 1$ und $-Q(y)$ ist ein primitives Element von $F^\#$.
2. Wenn $p = 2$ ist, dann ist
 $(x, y) = 1, Q(x) = 1, Q(y) = b$ und $P(t) = t^2 + t + b$ ist ein irreduzibles Polynom über F .

Beweis Wegen (20.9) und dessen Beweis ist Q wenigstens ähnlich zu so einer Form.

Beh.: Formen, die ähnlich zu Q sind, sind sogar äquivalent zu Q .

Für (1) ist zu zeigen: Es existieren $a, b, c, d \in F$ mit

$$\lambda \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \quad \forall \lambda \in F^\#$$

Das ist äquivalent zu den drei Gleichungen:

$$\lambda = a^2 + \alpha b^2, \quad 0 = ac + \alpha bd, \quad \lambda \alpha = c^2 + \alpha d^2$$

1. α Nichtquadrat:

(a) λ Nichtquadrat: $\lambda = \alpha b^2, \lambda \alpha = c^2, a = 0, d = 0$

(b) λ Quadrat: $\lambda = a^2, \lambda \alpha = \alpha d^2, b = 0, c = 0$

2. α Quadrat:

$\exists \beta \in F$ mit $\alpha = \beta^2 \Rightarrow$ Nach **Hilfssatz 1** existieren $a, b, c, d \in F$, für die

$$\lambda = a^2 + (\beta b)^2 \quad \text{und} \quad \lambda \beta^2 = c^2 + (\beta d)^2$$

gilt. Zu zeigen bleibt $ac + \alpha bd = 0$, was man mit ähnlichen Mittel wie oben beweisen kann. (2) verläuft analog.

□

Sei im Folgenden $D = D_+$ eine hyperbolische Ebene und $Q = D_-$ ein 2-dimensionaler, definitiver orthogonaler Vektorraum über F .

Bezeichne $D^m Q^k$ die orthogonale direkte Summe von m hyperbolischen Ebenen D mit k definitiven Vektorräumen Q .

Satz 21.2 *Es gilt:*

1. D^m ist hyperbolischer Raum mit Wittindex m .
2. D^{m-1} besitzt Wittindex $m - 1$.
3. D^{2m} ist äquivalent zu Q^{2m} .
4. Jeder $2m$ -dimensionale orthogonale Raum über F ist äquivalent zu entweder D^m oder $D^{m-1}Q$.

Beweis

1. D ist hyperbolische Ebene und demzufolge ist D^m hyperbolischer Raum. Nach (19.3.4) gilt für einen total singulären Untervektorraum X von D^m : $\dim(X) \leq \frac{2m}{2} = m$. Diese Schranke wird auch angenommen (nehme das Erzeugnis von jedem zweiten Basisvektor der hyperbolischen Ebenen) \Rightarrow Wittindex von D^m ist m .

2. Sei $V \simeq D^{m-1}Q$, $D^{m-1} \simeq U$ und $Q \simeq U^\perp = W$. Also $V \simeq U \oplus U^\perp$. Ferner sei X maximaler total singulärer UVR von $U \xrightarrow{1} \dim(X) = m - 1$. Es gilt $X \oplus^\perp W \subseteq X^\perp$. Da aber $\dim(X \oplus^\perp W) = m - 1 + 2 = m + 1$ und $\dim(X^\perp) = \dim(V) - \dim(X) = 2m - (m - 1) = m + 1$, gilt sogar $X \oplus^\perp W = X^\perp$.

Sei nun $w \in W^\#$. Da W definit ist gilt $Q(w) \neq 0$.

Sei $x \in X$. Dann gilt $Q(x + w) = Q(x) + Q(w) + cf(x, w) = Q(w) \neq 0$.

Beh.: X ist maximaler total singulärer UVR von X^\perp .

Ann.: X ist kein maximaler total singulärer UVR von X^\perp .

$\Rightarrow \exists y \in X^\perp$, $y \notin X$ mit $\langle X, y \rangle$ total singulär $\Rightarrow y \in X \oplus^\perp W \Rightarrow$

$\exists x \in X, w \in W$ mit $y = x + w$. $\Rightarrow Q(y) = Q(x + w) \neq 0$.

Widerspruch zu $\langle X, y \rangle$ total singulär.

Bem.: $D^{m-1}Q$ und D^m sind nicht äquivalent, da sie verschiedene Wittindizes haben.

(Wenn es eine Isometrie zwischen beiden VR geben würde, so müssten sie auch den gleichen Wittindex haben, da nach (20.8.1) die Isometriegruppe transitiv auf den maximalen total singulären UVR operiert.)

3. siehe 4.

4. Induktion nach m .

IA: Sei $m = 1$. Dann gilt $V \simeq D$, wenn V nicht definit ist (19.13) und $V \simeq Q$ andernfalls (21.1).

IV: Es gelte (21.2.4) für ein $m \in \mathbb{N}$.

IS: Sei V orthogonaler Raum von F mit $\dim(V) = 2m$.

Nach (20.11) besitzt V einen nichtsingulären UVR U mit $\dim(U) = 2$. Also: $V \simeq U \oplus U^\perp$.

Nach IV gilt $U^\perp \simeq D^{m-1}$ oder $U^\perp \simeq D^{m-2}Q$.

Also folgt $V \simeq D^m$, $V \simeq D^{m-1}Q$ oder $V \simeq D^{m-2}Q^2$.

Es bleibt zu zeigen, daß $Q^2 \simeq D^2$. Wegen (20.8.2) besitzt Q^2 eine eindeutige Zerlegung $H \oplus W$, wobei H maximaler hyperbolischer und W ein definitiver Raum ist. Nach (20.8.3) ist der Wittindex von Q^2 gegeben durch $\frac{\dim(H)}{2}$. Ist der Wittindex von Q^2 2, d.h. existiert ein 2-dimensionaler total singulärer UVR von Q^2 , dann folgt $\dim(H) = 4$, also $Q^2 \simeq D^2$.

Zu zeigen: Q^2 besitzt 2-dimensionalen total singulären UVR.

Es gilt $Q^2 = Q \oplus^\perp Q$. Sei $U \simeq Q$, dann gilt $U^\perp \simeq Q$.

Seien $\{x, y\}$ und $\{u, v\}$ Basen für U und U^\perp .

- i. $\text{char}(F) = 2$:

(21.1.2): $(x, y) = (u, v) = 1$, $Q(x) = Q(u) = 1$ und $Q(y) = Q(v)$
 $\langle x + u, y + v \rangle$ ist total singuläre Ebene, denn:

$$(x + u, x + u) = (x, x) + (u, u) = 1 + 1 = 2 = 0$$

$$(x + u, y + v) = (x, y) + (u, v) = 1 + 1 = 2 = 0$$

$$(y + v, y + v) = (y, y) + (v, v) = 2Q(y) = 0$$

ii. $\text{char}(F) \neq 2$:

$$(21.1.1): (x, y) = (u, v) = 0, -Q(x) = Q(u) = 1 \text{ und } -Q(y) = Q(v)$$

(Wähle die zu Q ähnliche Form $(-Q)(x) = -Q(x)$)

$\langle x + u, y + v \rangle$ ist total singuläre Ebene, denn:

$$(x + u, x + u) = (x, x) + (u, u) = Q(x) - Q(x) = 0$$

$$(x + u, y + v) = (x, y) + (u, v) = 0 + 0 = 0$$

$$(y + v, y + v) = (y, y) + (v, v) = Q(y) - Q(y) = 0$$

□

Wenn F endlich und n gerade, dann gibt es zwei quadratische Formen auf V .

$$\text{sgn}(Q) = \text{sgn}(V) := \begin{cases} +1, & \text{wenn } V \simeq D^m \\ -1, & \text{wenn } V \simeq D^{m-1}Q \end{cases} \text{ gibt den Isometrietyp an.}$$

Wenden wir uns nun dem Fall zu, wenn n ungerade ist. Nach (19.17) wissen wir bereits, daß dann $\text{char}(F)$ ungerade sein muß ($\text{char}(F) = 2 \Rightarrow \dim(V) = 2m + \text{Kontraposition}$).

Satz 21.3 Sei V ein orthogonaler Raum mit ungerader Dimension über einem endlichen Körper F . Dann besitzt V eine hyperbolische Hyperebene.

Beweis Induktion nach n .

IA: Sei $n = 1$. Nullraum

Sei $n = 3$. Nach (20.8.2) existiert eine eindeutige Zerlegung von V in $H \oplus W$, wobei H maximaler hyperbolischer und W ein definitiver Raum ist. Ist V nicht definit, so ist $\dim(H) = 2$ und H hyperbolische Hyperebene.

Zu zeigen: Es existiert ein singulärer Vektor von V .

Sei $\{v_1, v_2, v_3\}$ OGB von V (19.9). O.B.d.A. gilt entweder $(v_i, v_i) = 1$ oder $(v_i, v_i) = k$ für ein vorgegebenes Nichtquadrat k aus F ($i = 1, 2, 3$).

Da $n = 3$ gilt o.B.d.A. $(v_1, v_1) = (v_2, v_2)$.

Hilfssatz 1 sagt aus, daß $x^2 + y^2 = -\frac{(v_3, v_3)}{(v_1, v_1)}$ mit geeigneten $x, y \in F$.

Dann ist $xv_1 + yv_2 + v_3$ singulär, wegen

$$(xv_1 + yv_2 + v_3, xv_1 + yv_2 + v_3) = x^2(v_1, v_1) + y^2(v_2, v_2) + (v_3, v_3) = \underbrace{(x^2 + y^2)(v_1, v_1)}_{-(v_3, v_3)} + (v_3, v_3) = 0.$$

IV: Es gelte (21.3) für ein ungerades n .

IS: Nach (19.9) besitzt V einen UVR U mit $\text{codim}(U) = 2$, der n.a. ist. Sei $n > 3$. Nach IV besitzt U eine hyperbolische Hyperebene K . Es gilt $\dim(K^\perp) = n - \dim(K) = n - (n - 3) = 3$. Nach IV besitzt K^\perp eine

hyperbolische Ebene W . Betrachte $K \oplus W$.

$\dim(K \oplus W) = n - 3 + 2 = n - 1$ und $K \oplus W$ hyR, da K hyR und W hyE. Also ist $K \oplus W$ hyperbolische Hyperebene.

□

Satz 21.4 Sei F ein Körper mit $\text{char}(F)$ ungerade, n ungerade und c ein Erzeuger der multiplikativen Gruppe $F^\#$ von F . Dann gilt:

1. Es existieren (bis auf Äquivalenz) genau zwei n.a. quadratische Formen Q und cQ auf einem n -dimensionalen VR V über F .
2. Q und cQ sind ähnlich zueinander durch die skalare Transformation cI , d.h. $O(V, Q) = O(V, cQ)$.

Beweis Sei V ein orthogonaler VR mit ungerader Dimension über F .

$\Rightarrow V$ besitzt nach (21.3) eine hyperbolische Hyperebene H .

$\Rightarrow H$ ist nach (20.8) eindeutig bestimmt (bis auf Äquivalenz).

$\Rightarrow H^\perp$ ist dann ebenfalls eindeutig bestimmt (bis auf Äquivalenz).

Sei x ein Erzeuger von H^\perp .

Dann ist also x bis auf ein skalares Vielfaches eindeutig bestimmt. (*)

Definiere

$$\text{sgn}(Q) = \text{sgn}(V) := \begin{cases} +1, & \text{wenn } Q(x) \text{ Quadrat} \\ -1, & \text{wenn } Q(x) \text{ Nichtquadrat} \end{cases}$$

Haben zwei VR unterschiedliche Vorzeichen, so können sie nicht äquivalent sein.

Das sieht man so ein: Existiert eine Isometrie zwischen beiden VR, dann gilt wegen (*) $Q(x) = Q(bx) = b^2Q(x)$ für ein $b \in F$. Das bedeutet aber, die Vorzeichen müssen gleich sein.

Da c ein Erzeuger von $F^\#$ ist, ist c ein Nichtquadrat.

Sei $\text{sgn}(Q) = +1$. $\Rightarrow Q(x)$ ist Quadrat $\Rightarrow (cQ)(x) = cQ(x)$ ist Nichtquadrat $\Rightarrow \text{sgn}(cQ) = -1$.

Sei $\text{sgn}(Q) = -1$. $\Rightarrow Q(x)$ ist Nichtquadrat $\Rightarrow (cQ)(x) = cQ(x)$ ist Quadrat $\Rightarrow \text{sgn}(cQ) = +1$.

$\Rightarrow \text{sgn}(Q) \neq \text{sgn}(cQ) \Rightarrow (1)$

$(cQ)(x) = cQ(x) = \lambda(\alpha)Q(\alpha x)$ ist offensichtlich für $\alpha = id$ und $\lambda(\alpha) = c$ erfüllt.

Ausserdem gilt:

$\alpha \in O(V, Q) \Leftrightarrow Q(x) = Q(\alpha x) \Leftrightarrow cQ(x) = (cQ)(x) = (cQ)(\alpha x) = cQ(\alpha x) \Leftrightarrow \alpha \in O(V, cQ)$, was (2) bringt. □

Satz 21.5 Sei F ein endlicher Körper mit quadratischer Ordnung, also $|F| = p^2$. Dann existiert (bis auf Äquivalenz) genau eine unitäre Form f und (V, f) besitzt ONB.

Beweis Wegen $|F| = p^2$ gilt: $F = \mathbb{F}_{p^2}$ und $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = Z_2 = \langle \theta : a \rightarrow a^p \rangle$.

Zu zeigen: $F^\theta = \{aa^\theta \mid a \in F\} =: G$, denn dann folgt die Behauptung mit (19.11).

' \supseteq ': Sei $aa^\theta \in G \Rightarrow (aa^\theta)^\theta = (a^\theta)^\theta a^\theta = aa^\theta$. Also $aa^\theta \in F^\theta$.

' \subseteq ': Es gilt $F^\theta = \mathbb{F}_p$. Da die multiplikative Gruppe eines endlichen Körpers zyklisch ist, gilt: $F^\# = Z_{p^2-1}$ und $(F^\theta)^\# = (\mathbb{F}_p)^\# = Z_{p-1}$.

Ausserdem ist $(\mathbb{F}_p)^\#$ die Untergruppe von $F^\#$ mit $p-1$ Elementen, da zu jedem Teiler t der Ordnung einer zyklischen Gruppe genau eine Untergruppe der Ordnung t existiert. Sei also $F^\# = \langle a \rangle$. Betrachte $\text{ord}(a^{p+1})$. Es gilt

$\text{ord}(a^{p+1}) = \frac{p^2-1}{\text{ggT}(p+1, p^2-1)} = \frac{p^2-1}{p+1} = p-1$. (Ist H eine Gruppe und $\alpha \in H$ ein Element der endlichen Ordnung n , so gilt für jedes $k \in \mathbb{Z}$: $\text{ord}(\alpha^k) = \frac{n}{\text{ggT}(k, n)}$)

D.h. aber, daß a^{p+1} ein primitives Element von $(\mathbb{F}_p)^\#$ ist, also $(\mathbb{F}_p)^\# = \langle a^{p+1} \rangle$.

Sei nun also $b \in (F^\theta)^\#$.

$\Rightarrow \exists m \in \mathbb{N} : b = (a^{p+1})^m = (a^m)^{p+1} = a^m(a^m)^p = a^m(a^m)^\theta \in G$.

□

Als Zusammenfassung dieses Kapitels dient der letzte Satz:

Satz 21.6 Sei V ein n -dimensionaler VR über einem endlichen Körper q -ter Ordnung und Charakteristik p . Dann gilt:

1. Auf V existiert eine symplektische Form gdw. n gerade ist. In diesem Fall ist diese Form (bis auf Äquivalenz) eindeutig bestimmt und (V, f) ist ein hyperbolischer Raum. (19.16)
2. Auf V existiert eine unitäre Form, falls q ein Quadrat ist. In diesem Fall ist diese Form (bis auf Äquivalenz) eindeutig bestimmt und (V, f) besitzt eine ONB. (21.5)
3. Wenn n gerade ist, dann existieren genau zwei n.a. quadratische Formen. Zwei Formen sind genau dann äquivalent, wenn sie dasselbe Vorzeichen besitzen. Wenn P eine quadratische Form auf V ist, so ist P entweder isometrisch zu $D^{\frac{n}{2}}$ oder zu $D^{\frac{n}{2}-1}Q$ mit Vorzeichen $+1$ bzw. -1 . (21.2)
4. Wenn n ungerade ist, dann existiert eine n.a. quadratische Form gdw. p ungerade ist. In diesem Fall gibt es wieder zwei Äquivalenzklassen von Formen. Alle Formen sind ähnlich. (19.17)+(21.4)